

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-259012

(43)Date of publication of application : 16.09.1994

(51)Int.Cl.

G09C 1/00

H04L 9/06

H04L 9/14

(21)Application number : 05-070824

(71)Applicant : HITACHI LTD

HITACHI CHUBU SOFTWARE LTD

(22)Date of filing : 05.03.1993

(72)Inventor : SUZAKI SEIICHI

TAKARAGI KAZUO

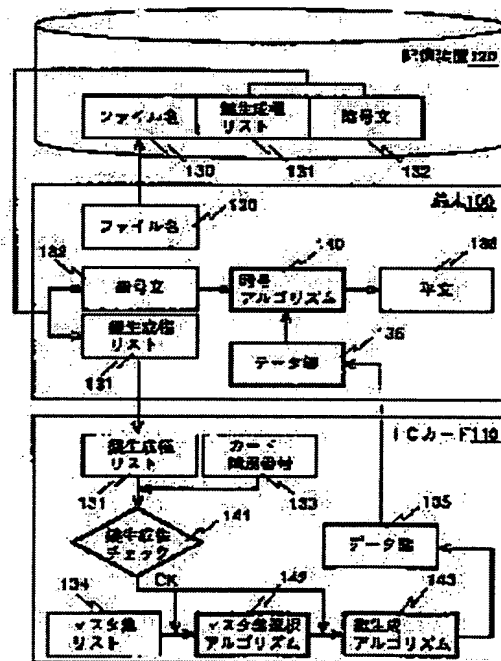
MATSUMOTO HIROSHI

## (54) ENCRYPTING METHOD BY HIERARCHIC KEY CONTROL AND INFORMATION COMMUNICATION SYSTEM

### (57)Abstract:

**PURPOSE:** To improve the safety of a file that plural users shares in environment where users are hierarchically sectioned according to kinds of information which can be accessed and to correctly decode a ciphertext file, controlled by a user belonging to one layer, by a user belonging to a layer above the layer.

**CONSTITUTION:** A terminal 100 reads a key generation right list 131 and a ciphertext 132, making a group with a file name 130 that the user inputs, out of a storage device 120 and sends only the key generation right list 131 to an IC card 110. When the received key generation right list 131 and the card identification number 133 of an IC card 110 satisfy specific relation, the IC card 110 generates a data key 135 on the basis of a master key selected from among the key generation right list 131 and its card master key list 134 and sends the data key to the terminal 100. The terminal 100 decodes the ciphertext 132 with the received data key 135 to generate a plaintext 136.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]



(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-259012

(43)公開日 平成6年(1994)9月16日

(51)Int.Cl.<sup>5</sup>

G 0 9 C 1/00

H 0 4 L 9/06

9/14

識別記号

庁内整理番号

8837-5L

F I

技術表示箇所

7117-5K

H 0 4 L 9/ 02

Z

審査請求 未請求 請求項の数17 F D (全 24 頁)

(21)出願番号

特願平5-70824

(22)出願日

平成5年(1993)3月5日

(71)出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71)出願人 000233457

日立中部ソフトウェア株式会社

愛知県名古屋市中区栄3丁目10番22号

(72)発明者 洲崎 誠一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(72)発明者 宝木 和夫

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

(74)代理人 弁理士 矢島 保夫

最終頁に続く

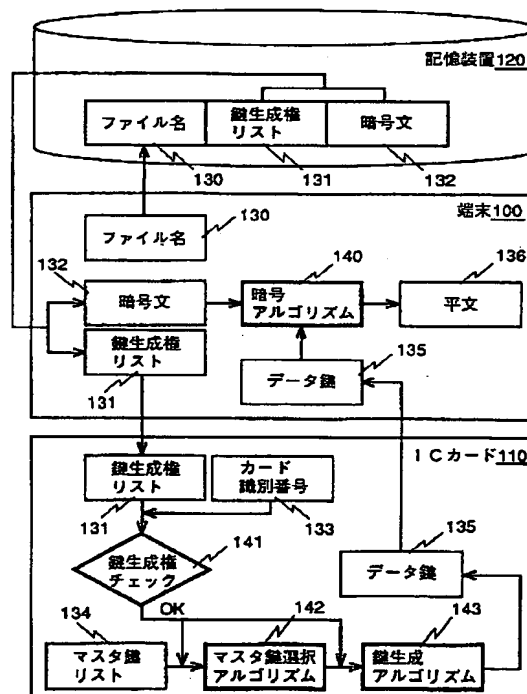
(54)【発明の名称】 階層型鍵管理による暗号方法及び情報通信システム

(57)【要約】

(修正有)

【目的】アクセスできる情報の種類によってユーザが階層的に区分される環境において、複数のユーザによって共有されるファイルの安全性を高める。また、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができる。

【構成】端末100は、ユーザが入力したファイル名130と組になっている鍵生成権リスト131及び暗号文132を記憶装置120より読み取り、鍵生成権リスト131だけをICカード110に送る。ICカード110は、受け取った鍵生成権リスト131及び自カード識別番号133がある特定の関係を満たすときは、鍵生成権リスト131、及び自カードマスタ鍵リスト134から選択したマスタ鍵とに基づいて、データ鍵135を生成し端末100に送る。端末100は受け取ったデータ鍵135で暗号文132を復号して平文136を生成する。



## 【特許請求の範囲】

【請求項1】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行ない、ある端末による上記記憶装置からのファイルの読出しは、

指定されたファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取るステップと、読み取った鍵生成権リストを、その端末に接続された記憶媒体に送信するステップと、

該記憶媒体において、受信した鍵生成権リストに自記憶媒体識別番号が含まれているか、またはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にあるか、を検査するステップと、該検査ステップにより、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかまたはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にある場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

【請求項2】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、

該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行なうことを特徴とする暗号方法。

【請求項3】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの読出し及び復号を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

あらかじめ上記記憶装置には、複数のユーザによって共有されるファイルのファイル名、当該ファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リスト、及び該鍵生成権リストと該鍵生成権リストにより選択されたマスタ鍵とに基づいて生成されたデータ鍵で暗号化された暗号文ファイルが、記憶されており、ある端末による上記記憶装置からのファイルの読出しは、

指定されたファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取るステップと、読み取った鍵生成権リストを、その端末に接続された記憶媒体に送信するステップと、

該記憶媒体において、受信した鍵生成権リストに自記憶媒体識別番号が含まれているか、またはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にあるか、を検査するステップと、該検査ステップにより、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかまたはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にある場合は、該鍵生成権リストに

10

20

30

40

50

基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、  
該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

【請求項4】請求項1ないし3のいずれかに記載の暗号方法において、  
前記記憶媒体が、ICカードであることを特徴とする暗号方法。

【請求項5】請求項1または3のいずれかに記載の暗号方法において、  
すべてのユーザは、アクセスすることができる情報の種類や重要度によって階層的に区分されているとともに、前記記憶媒体識別番号は、その記憶媒体を所有するユーザの階層が分かるように設定されており、  
前記検査ステップにおける所定の関係は、自記憶媒体識別番号が示す階層が、前記鍵生成権リストに含まれている記憶媒体識別番号が示す階層の上位階層である、という関係であることを特徴とする暗号方法。

【請求項6】請求項1ないし3のいずれかに記載の暗号方法において、  
前記記憶媒体識別番号が、その記憶媒体のユーザと他のユーザとの関係を表すことを特徴とする暗号方法。

【請求項7】請求項1または2のいずれかに記載の暗号方法において、  
前記記憶装置へのファイルの書き込み時に、データ鍵を生成して端末に返送するステップは、前記受信した鍵生成権リストに自記憶媒体識別番号が含まれているときにのみ、データ鍵の生成と端末への返送を行なうことを特徴とする暗号方法。

【請求項8】請求項5に記載の暗号方法において、  
前記記憶媒体中のマスタ鍵リストが、各ユーザ階層毎に異なる秘密数値であるマスタ鍵のうち、その記憶媒体を所有するユーザが属する階層のマスタ鍵及びその下位階層のマスタ鍵によって構成されることを特徴とする暗号方法。

【請求項9】請求項8に記載の暗号方法において、  
前記記憶装置へのファイルの書き込み時または読出し時に、前記記憶媒体内部でデータ鍵を生成する場合に、前記鍵生成権リストに記憶媒体識別番号が含まれるユーザが属する階層のうち、最も下位階層のマスタ鍵を選択して使用することを特徴とする暗号方法。

【請求項10】通信網によって相互に接続された複数の端末と該複数の端末からアクセス可能な記憶装置とを備えた情報通信システムにおいて、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう暗号方法であって、

上記端末は、あらかじめユーザに配布される演算機能を備えた記憶媒体であって、その記憶媒体に固有の記憶媒

体識別番号および複数のマスタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストを記憶した記憶媒体を、接続可能とし、

上記記憶装置への、ある端末からのファイルの書き込みは、

書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成するとともに、該鍵生成権リストの記憶媒体識別番号と所定の関係にある記憶媒体識別番号を算出して該鍵生成権リストに追記し、追記した鍵生成権リストを、端末からその端末に接続された記憶媒体に、送信するステップと、

該記憶媒体において、受信した鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成するステップと、  
該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込むステップとにより行ない、  
ある端末による上記記憶装置からのファイルの読出しは、

指定されたファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取るステップと、  
読み取った鍵生成権リストを、その端末に接続された記憶媒体に送信するステップと、

該記憶媒体において、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかを検査するステップと、  
該検査ステップにより、受信した鍵生成権リストに自記憶媒体識別番号が含まれている場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送するステップと、

該端末において、該データ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成するステップとにより行なうことを特徴とする暗号方法。

【請求項11】請求項2に記載の暗号方法において、  
前記記憶装置へのファイルの書き込み時の鍵生成権リストの生成の際、書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成するとともに、該鍵生成権リストの記憶媒体識別番号と所定の関係にある記憶媒体識別番号を算出して該鍵生成権リストに追記することを特徴とする暗号方法。

【請求項12】請求項5に記載の暗号方法において、  
前記記憶媒体中のマスタ鍵リストが、各ユーザ階層毎に異なる秘密数値であるマスタ鍵のうち、その記憶媒体を所有するユーザが属する階層のマスタ鍵である階層別マスタ鍵のみによって構成されることを特徴とする暗号方法。

【請求項13】請求項12に記載の暗号方法において、  
前記記憶装置へのファイルの書き込み時または読出し時

10

20

30

40

50

に、前記憶媒体内部でデータ鍵を生成する場合に、前鍵生成権リストに記憶媒体識別番号が含まれるユーザが属する階層のうち最も下位階層のマスタ鍵を、前記階層別マスタ鍵から算出して使用することを特徴とする暗号方法。

【請求項14】請求項1ないし3のいずれかに記載の暗号方法において、

さらに前記各記憶媒体は、その記憶媒体の所有者の個人識別番号を記憶しており、記憶媒体内部でデータ鍵を算出する場合に、該記憶媒体識別番号と個人識別番号とを  
10 使って、データ鍵を算出する権利があるかどうかを検査することを特徴とする暗号方法。

【請求項15】通信網によって相互に接続された複数の端末と、該複数の端末からアクセス可能な記憶装置と、該端末に接続可能であってあらかじめユーザに配布される演算機能を備えた記憶媒体とを備え、複数のユーザによって共有される上記記憶装置上のファイルの暗号化を行なう情報通信システムであって、

上記記憶媒体は、

その記憶媒体に固有の記憶媒体識別番号および複数のマ  
20 スタ鍵とよばれる秘密数値によって構成されたマスタ鍵リストと、

上記記憶装置へのファイルの書き込み処理において端末から送信された鍵生成権リストを受信し、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送する手段と、

上記記憶装置からのファイルの読出し処理において端末から送信された鍵生成権リストを受信し、該鍵生成権リストに自記憶媒体識別番号が含まれているか、またはそ  
30 の鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にあるか、を検査する手段と、

該検査手段により、受信した鍵生成権リストに自記憶媒体識別番号が含まれているかまたはその鍵生成権リストに含まれている記憶媒体識別番号と自記憶媒体識別番号とが所定の関係にある場合は、該鍵生成権リストに基づいてマスタ鍵を選択し、該選択したマスタ鍵と受信した鍵生成権リストとに基づいてデータ鍵を生成して、端末に返送する手段とを備え、

上記端末は、

上記記憶装置へのファイルの書き込み処理において、書き込むファイルの共有者を表す記憶媒体識別番号のリストである鍵生成権リストを生成し、該鍵生成権リストを上記記憶媒体に送信する手段と、

上記記憶媒体から返送されたデータ鍵を用いて平文ファイルを暗号化して、暗号文ファイルを生成する手段と、該暗号文ファイル、鍵生成権リスト、及びファイル名を、上記記憶装置に書き込む手段と、

上記記憶装置からのファイルの読出し処理において、読  
50

出すファイルのファイル名に応じて、上記記憶装置から暗号文ファイルと鍵生成権リストとを読み取る手段と、読み取った鍵生成権リストを、上記記憶媒体に送信する手段と、

上記記憶媒体から返送されたデータ鍵を用いて暗号文ファイルを復号して、平文ファイルを生成する手段とを備えたことを特徴とする情報通信システム。

【請求項16】演算手段と、リーダライタインタフェースと、記憶手段とを備え、該記憶手段にはそのICカードに固有のICカード識別番号を記憶したICカードにおいて、

上記リーダライタインタフェースを介してICカード識別番号のリストを受信したとき、該リストに自ICカード識別番号が含まれていたらデータ鍵を生成して出力するとともに、該リストに自ICカード識別番号が含まれていない場合であっても、該リストに含まれているICカード識別番号と自ICカード識別番号とが所定の条件を満足する場合にはデータ鍵を生成して出力することを特徴とするICカード。

【請求項17】演算手段と、リーダライタインタフェースと、記憶手段とを備えたICカードにおいて、

上記記憶手段には、一般の用途に使用されるカード所有者の個人識別番号のほかに、暗号に使用するための識別番号を記憶していることを特徴とするICカード。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、例えば会社組織のように、アクセスできる情報の種類や重要性によってユーザを階層的に分けることができるような環境において、複数のユーザによって共有される情報を適式に暗号化することができる暗号方法及びそのような暗号方法を適用した情報通信システムに関し、更に詳しくは、ある階層に属するユーザによって管理されている暗号化された情報を、その上位階層に属するユーザも正しく復号することができる暗号方法及び情報通信システムに関する。

【0002】

【従来の技術】情報通信機器の発達により、ワークステーションやパソコン等を端末としたローカルエリアネットワーク（LAN）が広く用いられるようになってきている。これに伴い、様々な情報が電子化されて送られるようになってきている。

【0003】LANでは、情報は回線を同報的に流れている。すなわち、情報の送信元は、送信すべき情報に相手先のアドレスを付して回線に送信し、回線上のすべての端末でこれを受信する。受信した端末側では、アドレスを参照して、自己へ向けて送信された情報であるかどうかをチェックする。したがって、ある端末が同報的に送出した情報は、基本的にどの端末でも受信可能である。そのため、機密性の高い情報を送信する場合には、暗号化やアクセス制御といったセキュリティ技術を使つ

て情報の保護を行っている。

【0004】一方、このような環境下では、複数のユーザが共同で作業するために、ファイルの共有といったことも行われる。複数のユーザによって共有されるファイルは各個人毎のファイルと比べて、正しい内容が第三者に漏洩した場合に、その影響が一度に多くのユーザに波及する。したがって、このようにファイルとして蓄積される情報についても、通信回線を送られる情報と同様に、暗号やアクセス制御といったセキュリティ技術を使って、きちんと保護する必要がある。

【0005】通信回線を送られる情報を暗号化する場合、あるいはファイルとして蓄積される情報を暗号化する場合には、通信者間、あるいはファイルを共有するユーザ間で暗号鍵を共有する必要がある。

【0006】ところが、ファイルとして蓄積される情報を暗号化する場合には、次のような課題が生じる。

【0007】それは、通信回線を送られる情報を暗号化する場合に暗号鍵を1セッション毎に使い捨てにすることができるが、ファイル情報を暗号化する場合には、その暗号文をいつ復号するかわからないので、暗号鍵も暗号文と一緒に保存しておかなければならないということである。

【0008】ファイルを適式に暗号化する方法については、例えば「暗号と情報セキュリティ（編著：辻井 重雄，笠原 正雄；発行：昭晃堂）」に開示されている。

【0009】上記開示例では、まずランダムに生成した乱数でファイルを暗号化して暗号文ファイルを生成する。更に、その乱数もマスタ鍵と呼ばれるシステム固有の秘密数値で暗号化し、暗号文鍵（暗号化された暗号鍵）を生成する。そして、この暗号文鍵を暗号文ファイルとを合わせて記憶しておく。ファイルを読み取る場合には、まず暗号文鍵をマスタ鍵で復号してから暗号文ファイルを復号する。

【0010】その際、暗号文ファイルを復号して正しい内容を読み取る権利があるかどうかのチェックは、別途ファイルのアクセス制御（そのファイルをアクセスする権利がある者かどうかをチェックする方法）によってのみ行っている。

【0011】

【発明が解決しようとする課題】ところで、例えば、図21のような会社組織では、アクセスできる情報の種類や重要性によってユーザを階層的に区分することができる。このような環境においては、部下の作成したファイルは上司も読み取ることができるが、上司の作成したファイルは部下の側から読み取ることができないようにしたいといった要求がある。

【0012】しかし、上記従来技術では、正しい内容を読み取る権利があるかどうかのチェックをアクセス制御によってのみ行っているため、上司は自分より下位に属するすべての部下のマスタ鍵を知っていなければなら

い。そうでないと、部下が暗号化したファイルを復号できないからである。しかし、すべての部下のマスタ鍵を管理するのでは、ユーザの負担が大き過ぎる。また、パソコンのようにアクセス制御機能を持たない端末には、適用できないといった問題点がある。

【0013】そこで、本発明の一つの目的は、複数のユーザによって共有されるファイルを、ユーザにあまり負担をかけることなく適式に暗号化して安全性を高めることができる暗号方法及び装置を提供することにある。

10 【0014】本発明のもう一つの目的は、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができるような暗号方法及び装置を提供することにある。

【0015】

【課題を解決するための手段】上記目的を達成するため、第1の観点では、本発明は、まず各ユーザに配布された記憶媒体（例えば、ICカード）の識別番号によって、暗号鍵を生成する権利があるかどうかのチェックを行ない、その結果にしたがって暗号鍵を生成することを特徴とする暗号方式を提供する。

【0016】第2の観点では、本発明は、暗号文ファイルを復号する場合に、あらかじめファイル作成者に許可されたユーザかどうかをチェックするだけでなく、そのユーザの上位階層に属するユーザかどうかのチェックをも行なうことを特徴とする暗号方式を提供する。

【0017】第3の観点では、本発明は、暗号鍵生成に使用されるマスタ鍵をユーザ階層毎に用意し、各ユーザに対して、そのユーザが属する階層とその下位階層のマスタ鍵を配布することを特徴とする暗号方式を提供する。

【0018】

【作用】上記第1の観点による暗号方式では、複数のユーザによって共有されるファイルを、ユーザにあまり負担をかけることなく適式に暗号化することができる。

【0019】上記第2の観点による暗号方式では、暗号鍵を生成する権利があるかどうかということを判定する際に、ファイル作成者に許可されたユーザの上位階層に属するユーザかどうかのチェックも行なっているため、ある階層に属するユーザによって管理されている暗号文ファイルを、その上位階層に属するユーザも正しく復号することができる。

【0020】上記第3の観点による暗号方式では、ユーザは自分が属する階層より上位階層のマスタ鍵を手に入れることができないので、ある階層に属するユーザによって管理されている暗号文ファイルを、その下位階層に属するユーザが正しく復号することはできない。

【0021】

【実施例】以下、図面を用いて、本発明の実施例を説明する。なお、以下で説明する図面において、同一の番号は同様の部品・要素を表すものとする。これにより本発

明が限定されるものではない。

【 0 0 2 2 】 ( 実施例 1 )

【 0 0 2 3 】 図 1 は、本発明の第 1 の実施例であり、本発明に係る暗号方法を適用したシステムにおける暗号文 ( ファイル情報 ) の復号の手順を示すブロック図である。図 2 は、本実施例のシステムのシステム構成を示すブロック図である。

【 0 0 2 4 】 まず、図 2 を参照して、本実施例のシステム構成を説明する。

【 0 0 2 5 】 図 2 において、1 0 0、1 0 1 はワークステーションやパソコン等の端末である。ユーザは、これらの端末を使って種々の作業を行なう。1 2 0 は通信網 2 1 0 によって端末 1 0 0、1 0 1 と接続された記憶装置である。ユーザは、アプリケーションプログラムを使って作成したファイル等を、この記憶装置 1 2 0 に記憶させることができる。また、記憶装置 1 2 0 の情報を読み出すことができる。

【 0 0 2 6 】 1 1 0、1 1 1 は、あらかじめ各ユーザに対してそれぞれ 1 枚ずつ配布されている IC カードである。ユーザは、自己の IC カードをリーダライタ 2 0 0、2 0 1 に差し込んで、作業を行なう。IC カード 1 1 0、1 1 1 は、リーダライタ 2 0 0、2 0 1 を介して、端末 1 0 0、1 0 1 とデータのやり取りを行なう。

【 0 0 2 7 】 図 3 は、端末 1 0 0 の内部構成図である。端末 1 0 1 など他の端末も同様の構成である。同図に示すように、端末 1 0 0 は、通信網インタフェース 3 0 1 と、リーダライタインタフェース 3 0 2 と、CPU ( 中央処理装置 ) 3 0 3 と、表示装置 3 0 4 と、入力装置 3 0 5 と、メモリ 3 0 6 とを有している。それらは、バス 3 0 0 によって相互に接続されている。

【 0 0 2 8 】 通信網インタフェース 3 0 1 は、通信網 2 1 0 を介して記憶装置 1 2 0 とデータのやり取りを行なう際のインタフェースである。リーダライタインタフェース 3 0 2 は、ケーブル 3 1 0 を介してリーダライタ 2 0 0 との間でデータのやり取りを行なうためのインタフェースである。CPU 3 0 3 は、演算機能を備え、この端末全体の動作を制御する。表示装置 3 0 4 は、ユーザにメッセージを表示するためのディスプレイ等である。入力装置 3 0 5 は、ユーザがデータを入力するためのキーボードやマウス等である。メモリ 3 0 6 には、通信プログラム 3 0 7、アプリケーションプログラム 3 0 8、およびセキュリティプログラム 3 0 9 等が記憶されている。

【 0 0 2 9 】 メモリ 3 0 6 に記憶されている通信プログラム 3 0 7 は、記憶装置 1 2 0 やリーダライタ 2 0 0 との間でデータのやり取りを行なう際にそれを制御するプログラムである。アプリケーションプログラム 3 0 8 は、ユーザが新規ファイルの作成や既存ファイルの読み取り、書き込み等を行なう際にそれを支援・制御するプログラムである。また、セキュリティプログラム 3 0 9

は、ファイルの暗号化及び復号に係る種々の処理を行なうプログラムである。

【 0 0 3 0 】 図 4 は、IC カード 1 1 0 の内部構成図である。IC カード 1 1 1 など他の IC カードの構成も同様である。同図に示すように、IC カード 1 1 0 は、CPU 4 0 1 と、リーダライタインタフェース 4 0 2 と、メモリ 4 0 3 とを有している。それらはバス 4 0 0 によって相互に接続されている。

【 0 0 3 1 】 CPU 4 0 1 は、演算機能を備え、IC カード内の処理の全体を制御する。リーダライタインタフェース 4 0 2 は、リーダライタ 2 0 0 との間でデータのやり取りを行なうためのインタフェースである。メモリ 4 0 3 には、通信プログラム 4 0 4、セキュリティプログラム 4 0 5、マスタ鍵リスト 4 0 6、及びカード識別番号 4 0 7 等が記憶されている。

【 0 0 3 2 】 メモリ 4 0 3 に記憶されている通信プログラムは、リーダライタ 2 0 0 との間でデータのやり取りを行なう際にそれを制御するプログラムである。セキュリティプログラム 4 0 5 は、リーダライタ 2 0 0 を介して端末 1 0 0 から送られてきた情報をもとに暗号鍵を生成する際の種々の処理を行なうプログラムである。

【 0 0 3 3 】 マスタ鍵リスト 4 0 6 は、各ユーザ階層毎に共通の秘密数値であるマスタ鍵のうち、IC カード 1 1 0 の所有者が属している階層及びその下位階層のマスタ鍵によって構成される数値列である。

【 0 0 3 4 】 例えば、本実施例のシステムが適用される組織が、図 5 のような階層構造であったとする。A、B、C、…は組織を構成する各人を示し、上位にいる者が上司である。例えば、J ~ P の上司は F であり、E ~ G の上司は B である。このような組織の場合、第 2 階層に属する B が所有する IC カードのマスタ鍵リストの構成要素は、KM2、KM3、KM4 の三つである。すなわち、B の IC カードには、自己の階層のマスタ鍵 KM2 のほか、下位階層のマスタ鍵 KM3、KM4 も記憶されている。また、第 4 階層に属する M の IC カードのマスタ鍵リストの構成要素は、KM4 のみである。

【 0 0 3 5 】 再び図 4 を参照して、カード識別番号 4 0 7 は、IC カード 1 1 0 に固有の数値である。全ユーザが役職により図 5 のように構造化されている場合に、カード識別番号 4 0 7 は、IC カード 1 1 0 の所有者がどのノードに位置しているかということを示す。

【 0 0 3 6 】 また、すべての IC カードのカード識別番号は、例えば図 6 のような識別番号テーブル 6 0 0 といった形式で記憶装置 1 2 0 に記憶される。図 6 の識別番号テーブル 6 0 0 において、「氏名」はこの組織に属する IC カードを所有するものすべての氏名を示し、「役職」はその者の役職を示す。「個人識別番号」は、その個人に固有の識別番号 ( 例えば、職員番号のようなもの ) である。「カード識別番号」は、上記の IC カードのカード識別番号 4 0 7 の値である。

【0037】上述したように、カード識別番号によってそのICカードの所有者の組織内における位置（いわば役職）が分かるようになっている。例えば、図5の組織では全体で4階層あるから、図6のようにカード識別番号は4つの数値を並べて構成される。

【0038】カード識別番号は、左側から順に参照したときに、「0」が出現する位置で、そのカードが属する階層が分かる。例えば、Aの所有するICカードのカード識別番号は（1，0，0，0）であるが、左側から見ると第1番目の数値が「0」以外で「1」、次の第2番目の数値が「0」であるので、Aは第1階層に属することが分かる。また、Gの所有するICカードのカード識別番号は（1，1，3，0）であるが、第1番目の数値が「0」以外で「1」、次の第2番目の数値が「0」以外で「1」、次の第3番目の数値が「0」以外で「3」、次の第4番目に「0」が出現するから、Gは第3階層に属することが分かる。

【0039】さらに、「0」が出現する前までの数値で、組織内の位置が分かる。例えば、Cの所有するICカードのカード識別番号は（1，2，0，0）であるが、第1番目の数値「1」でこのカードの所有者が第1階層の第1番目の者（カード識別番号（1，0，0，0）の者）の部下であることが分かる。また、「0」が出現する前にある第2番目の数値「2」で、このカードの所有者がその部下のうちで第2番目の者（すなわち、図5のC）であることが分かる。同様に、例えば、Lのカード識別番号（1，1，2，3）により、このICカードの所有者が、カード識別番号（1，1，2，0）の者の部下であって、その部下のうちの第3番目の者であることが分かる。

【0040】次に、図1を参照して、本実施例において既に記憶装置120に記憶されている暗号文（暗号文ファイル）を復号する手順について簡単に説明する。

【0041】まず、ユーザは、読出したいファイルのファイル名130を入力する。端末100は、ユーザが入力したファイル名130を記憶装置120に送る。記憶装置120は、そのファイル名130と組になっている鍵生成権リスト131および暗号文132を、端末100へと送る。端末100は、読み取った鍵生成権リスト131および暗号文132のうち、鍵生成権リスト131だけをICカード110に送る。

【0042】鍵生成権リストとは、当該ファイルを読出し復号する権利のある者を示すカード識別番号のリストである。この実施例では、そのファイルに対するアクセス権を有する者を示すカード識別番号を連結した形式のデータであるが、別の形式で表現してもよい。アクセス権を有する者を示すカード識別番号が分かるようなデータであればよい。鍵生成権リストは、ファイルを作成した者がそのファイルを記憶装置120に書き込む際に生成され、記憶装置120に書き込まれるようになってい

る。誰にアクセス権を与えるかは、ファイルを作成した者が指定する。

【0043】ICカード110は、受け取った鍵生成権リスト131と自カード識別番号133とがある特定の関係を満たすかどうか、鍵生成権チェック141を行なう。特定の関係のチェックとは、自カード識別番号133が鍵生成権リスト131に指定されているかどうか、あるいは自カード識別番号133が鍵生成権リスト131に指定されている者の上司を示しているかどうか、に関するチェックである。言い換えると、鍵生成権リスト131に指定されているアクセス権を有する者であるか、あるいはその上司であるか、をチェックしている。

【0044】ICカード110は、鍵生成権チェック141において、鍵生成権リスト131と自カード識別番号133とが特定の関係を満たすときのみ、マスタ鍵選択アルゴリズム142を用いて自カードマスタ鍵リスト134からマスタ鍵を選択する。マスタ鍵選択アルゴリズム142は、鍵生成権リスト131でアクセス権を有すると指定されている者の階層をチェックし、最も下位の階層のマスタ鍵を、マスタ鍵リスト134の中から選択する。これは、上位の階層の者のICカードは下位階層のマスタ鍵まで記憶しているのに対し、下位の階層の者のICカードは上位階層のマスタ鍵を記憶していないことによる。すなわち、マスタ鍵を、アクセス権を有する者のうちの最も下位の階層に合せるということである。

【0045】次に、ICカード110は、鍵生成権リスト131と選択したマスタ鍵をもとにデータ鍵135を生成し、端末100に送る。

【0046】端末100は、受け取ったデータ鍵135を用いて、暗号アルゴリズム140により暗号文132を復号し、平文136を生成する。以上のように、平文136を得ることができる。

【0047】次に、図7から図10を参照して、本実施例におけるユーザの操作や端末100及びICカード110内部の処理について詳しく説明する。

【0048】図7は、平文ファイルを暗号化して記憶装置120に書き込む場合の処理手順を示す流れ図である。

【0049】本処理は、ユーザが自己のICカード110をリーダライタ200に挿入し、入力装置305を使って、アプリケーションプログラム308によって作成した平文ファイルを記憶装置120に書き込む操作をすることによって開始される（ステップ700）。

【0050】端末100は、まず記憶装置120内の識別番号テーブル600（図6）を読み取り、それを表示装置304に表示する（ステップ701）。ユーザは、表示された識別番号テーブル600を参照し、作成した平文ファイルの共有相手を入力装置305を使って指定する。端末100は、その指定されたすべてのユーザの

カード識別番号から成る鍵生成権リストを生成する(ステップ702)。そして、その鍵生成権リストをICカード110に送る(ステップ703)。

【0051】ICカード110は、端末100より送られてきた鍵生成権リストをもとに、データ鍵を生成し、端末100に送り返す(ステップ704)。なお、このICカード110の処理は、図8を参照して後述する。

【0052】端末100は、ICカード110より送られてきたデータ鍵を使って平文ファイルを暗号化する(ステップ705)。そして、その生成された暗号文ファイルとファイル名と鍵生成権リストとを組にして、記憶装置120に書き込む(ステップ706)。

【0053】最後に、ユーザがリーダライタ200よりICカード110を取り出すことによってすべての処理が終了する(ステップ707)。

【0054】図8は、図7におけるICカード110内部の鍵生成処理(ステップ704)を更に詳しく示した流れ図である。本処理は、ICカード110が端末100より鍵生成権リストを受け取ることによって開始される(ステップ800)。

【0055】ICカード110は、まず受け取った鍵生成権リストの構成要素に、自カード識別番号が含まれているかどうかを検査する(ステップ801)。含まれている場合には、ステップ802に進み、処理を続ける。含まれていない場合は、処理を終了する(ステップ804)。

【0056】受け取った鍵生成権リストの構成要素に自カード識別番号が含まれている場合、ICカード110は、その鍵生成権リストを参照し、その構成要素のうち最も下位のユーザ階層に割り当てられているマスタ鍵を、マスタ鍵リストの中から選択する(ステップ802)。そして、その選択されたマスタ鍵と鍵生成権リストとからデータ鍵を生成し、それを端末100に送り返す(ステップ803)。そして、すべての処理を終了する(ステップ804)。

【0057】図9は、記憶装置200に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順を示す流れ図である。

【0058】本処理は、ユーザがICカード110をリーダライタ200に挿入し、記憶装置120に記憶されている暗号文ファイルを読み取る操作をすることによって開始される(ステップ900)。

【0059】端末100は、まず記憶装置120に記憶されている各暗号文ファイルのファイル名を読み取り、そのファイル一覧を表示装置304に表示する(ステップ901)。

【0060】ユーザは、表示されたファイル名の一覧を参照し、読み込みたいファイル名を入力装置305を使って指定する。端末100は、その指定されたファイル名と組になって記憶されている暗号文ファイルと鍵生成

権リストとを記憶装置120から読み取る(ステップ902)。そして、鍵生成権リストのみをICカード110に送る(ステップ903)。

【0061】ICカード110は、端末100より送られてきた鍵生成権リストをもとにデータ鍵を生成し、端末100に送る(ステップ904)。なお、このICカード110の処理は、図10を参照して後述する。

【0062】端末100は、ICカード110より送られてきたデータ鍵を使って暗号文ファイルを復号する(ステップ905)。最後に、ユーザがリーダライタ200よりICカード110を取り出すことによって、すべての処理が終了する(ステップ906)。

【0063】図10は、図9におけるICカード内部の鍵生成処理(ステップ904)を更に詳しく示した流れ図である。図10の手順は、基本的に図8と同様であるので、同じ処理を行なうステップは同じ番号を付してある。

【0064】ただし、図10では、自カード識別番号が、端末100より受け取った鍵生成権リストに含まれているカード識別番号とある特定の関係を満たす場合にも、データ鍵を生成することを許している点が異なっている(ステップ1000、1001)。この場合のある特定の関係とは、ICカードの所有者が、鍵生成権リストにカード識別番号が含まれているユーザの上司であるという関係である。

【0065】例えば、図6に示すようにカード識別番号が割り当てられている場合、ICカード内のカード識別番号と鍵生成権リストに含まれているカード識別番号とがこの関係を満たすかどうかは、次のようにして検査される。すなわち、ICカード内のカード識別番号と鍵生成権リストに含まれているすべてのカード識別番号との排他的論理和をそれぞれ計算し、ICカードの所有者が属する階層までの数値を検査し、それらがすべて数値0ならば関係を満たしていると判定することができる。

【0066】これは、ある者(上司)の直属の部下のカード識別番号を、その上司のカード識別番号で左から見て初めて出現する「0」の位置に「1」「2」…を設定して構成するようにしているからである。例えば、図6のBのカード識別番号(1, 1, 0, 0)とGのカード識別番号(1, 1, 3, 0)との排他的論理和は(0, 0, 0, 0)となるから、BとCは上司と部下の関係にあると分かる。

【0067】上述の実施例では、ファイル作成者が指定したユーザ及びそれらユーザとある特定の関係にあるユーザ(例えば、上記で説明した例では上司)が、自分の所有するICカードを端末と接続したリーダライタに挿入した場合にのみ、ICカード内部で正しいデータ鍵が生成される。したがって、ICカードを持たない第三者やファイルを読み取る権利のないユーザは、正しい内容を知ることはできず、共有ファイルの安全性が高くな

る。

【 0 0 6 8 】 更に、ファイルを共有するであろう相手毎にあらかじめデータ鍵を共有しておくのではなく、鍵生成権リストやマスタ鍵リストから IC カード内部でその都度データ鍵を生成するので、ファイルを共有する相手が多いユーザの負担を軽減し、任意の相手と安全にファイル共有することができる。

【 0 0 6 9 】 ( 実施例 2 )

【 0 0 7 0 】 次に、本発明の第 2 の実施例を説明する。第 2 の実施例は、基本的には上述の第 1 の実施例と同様である。そのシステムのシステム構成、端末の内部構成、および IC カードの内部構成は、上述の第 1 の実施例の図 2、3、4 と同様であり、また暗号文 ( ファイル情報 ) の復号の手順も図 1 と同様である。さらに、識別番号テーブルの構成も図 6 と同様である。

【 0 0 7 1 】 上記第 1 の実施例では、図 7 の手順によって平文ファイルを暗号化して記憶装置 1 2 0 に書き込むが、第 2 の実施例では図 1 1 の手順を用いる。

【 0 0 7 2 】 図 1 1 を参照して、本実施例において平文ファイルを暗号化して記憶装置 1 2 0 に書き込む場合の処理手順を説明する。図 1 1 において、図 7 と同じ処理ステップには同じ番号を付し、説明は省略する。図 1 1 では、ステップ 1 1 0 0、1 1 0 1 が増えている。

【 0 0 7 3 】 すなわち、ステップ 1 1 0 0 で、入力装置 3 0 5 を使って指定されたユーザのカード識別番号と、ある特定の関係を満たすカード識別番号 ( 例えば、指定されたユーザの上司のカード識別番号 ) を、端末 1 0 0 においてあらかじめ生成する。そして、ステップ 1 1 0 1 で、そのカード識別番号を鍵生成権リストに追加する。追加した結果の鍵生成権リストを、ステップ 7 0 3 で IC カード 1 1 0 に送信するようにしている。

【 0 0 7 4 】 また、本実施例において、記憶装置 1 2 0 に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順は図 9 と同様である。また、IC カード内部の鍵生成処理は、ファイルの書き込み、読み取りいずれの場合にも図 8 と同様である。

【 0 0 7 5 】 第 1 の実施例では、ファイルの読出し時に特定の関係をチェックし、例えば上司にもそのファイルが読み出せるようにしていた。これに対し、本実施例では、あらかじめファイルを書き込む際に、特定の関係を満たすカード識別番号、例えば上司カード識別番号を、生成して鍵生成権リストに追加するようにしている。したがって、第 1 の実施例と同様の効果が得られるほかに、一般的にいうと端末より能力の劣る IC カード内部での処理を軽減し、より高速化を計ることができる。

【 0 0 7 6 】 ( 実施例 3 )

【 0 0 7 7 】 次に、本発明の第 3 の実施例を説明する。第 3 の実施例は、基本的には上述の第 1 の実施例と同様である。そのシステムのシステム構成、および端末の内部構成は、上述の第 1 の実施例の図 2、3 と同様であ

る。識別番号テーブルの構成も図 6 と同様である。

【 0 0 7 8 】 図 1 2 は、本実施例における暗号文 ( ファイル情報 ) の復号の手順の概略を示すブロック図である。図 1 2 において、図 1 と同じ処理あるいは情報には同じ番号を付して説明を省略する。図 1 2 が図 1 と異なる点は、ブロック 1 2 0 0、1 2 1 0 である。

【 0 0 7 9 】 すなわち、本実施例では、IC カード 1 1 0 において、マスタ鍵リストから必要なマスタ鍵を選択するのではなく、マスタ鍵生成アルゴリズム 1 2 1 0 を用いて階層別マスタ鍵 1 2 0 0 から必要とする階層別マスタ鍵を生成するという点が異なる。階層別マスタ鍵 1 2 0 0 とは、当該 IC カードの所有者が属する階層のマスタ鍵をいう。例えば、図 5 の組織では、A が所有する IC カードは階層別マスタ鍵として第 1 階層のマスタ鍵 KM 1 を記憶し、B が所有する IC カードは階層別マスタ鍵として第 2 階層のマスタ鍵 KM 2 を記憶している。

【 0 0 8 0 】 図 1 3 は、階層別マスタ鍵があらかじめ相互に関連付けて生成されており、上位階層のマスタ鍵から下位階層のマスタ鍵を生成できることを示す図である。すなわち、第 i 階層マスタ鍵 1 3 0 0 から一方向性関数 1 3 1 0 を用いて第 i + 1 階層マスタ鍵 1 3 0 1 を生成することができる。一方向性関数であるから、下位階層のマスタ鍵から上位階層のマスタ鍵を生成することはできない。

【 0 0 8 1 】 図 1 4 は、IC カードの内部構成を示すブロック図であり、これは基本的に図 4 と同じである。ただし、メモリ 4 0 3 にはマスタ鍵リストではなく、階層別マスタ鍵 1 4 0 0 が一つだけ記憶されている。なお、一方向性関数 1 3 1 0 はセキュリティプログラム 4 0 5 に備えられている。

【 0 0 8 2 】 図 1 5 は、ファイルの書き込み及び読み取り時の IC カード内部の鍵生成処理を示す流れ図である。これは基本的には図 8 と同じである。ただし、自カードの階層別マスタ鍵から必要となる階層別マスタ鍵を生成し ( ステップ 1 5 0 0 )、その生成された階層別マスタ鍵と鍵生成権リストとからデータ鍵を生成する ( ステップ 1 5 0 1 ) という点が異なる。

【 0 0 8 3 】 また、本実施例におけるファイルの書き込み及び読み取りの際の処理手順は、それぞれ図 1 1、図 9 と同様である。

【 0 0 8 4 】 本実施例によれば、第 1 及び第 2 の実施例と同様の効果が得られるほかに、IC カードに記憶しておかなければならない情報量を減らすことができ、区分されるユーザ階層が多い場合等において有効である。

【 0 0 8 5 】 ( 実施例 4 )

【 0 0 8 6 】 次に、本発明の第 4 の実施例を説明する。第 4 の実施例は、基本的には上述の第 3 の実施例と同様である。そのシステムのシステム構成、および端末の内部構成は、上述の第 1 の実施例の図 2、3 と同様である。識別番号テーブルの構成も図 6 と同様である。

10

20

30

40

50

【0087】図16は、本実施例における暗号文（ファイル情報）の復号の手順の概略を示すブロック図である。図16において、図12と同じ処理あるいは情報には同じ番号を付して説明を省略する。図12が図1と異なる点は、ブロック1600、1610、1601、1611である。

【0088】すなわち、本実施例では、鍵生成権のチェック141をする前に、ICカードの所有者が確かに識別番号テーブルに記載されているノード（役職）に位置しているかという使用権のチェック1611を行なう点が異なる。

【0089】図17は、ICカードの内部構成を示すブロック図であり、これは基本的に図14と同じである。ただし、メモリ403にはその他に、各ユーザごとに異なる数値である個人識別番号1700が記憶されている。

【0090】図18は、本実施例において、平文ファイルを暗号化して記憶装置120に書き込む場合の処理手順を示す流れ図である。これは基本的に図11と同じである。ただし、図11のステップ704が、ステップ1800、1801、1802に置き替わっている。

【0091】図18において、ステップ703で鍵生成鍵リストをICカードに送ると、ステップ1800でICカードはデータ鍵生成処理1を行なう。これは、後述する図20のステップ2000の処理であり、ICカードが自カード識別番号を端末に返送する処理である。

【0092】端末は、ステップ1801で、識別番号テーブル1600を参照して、ICカードから受け取ったカード識別番号と対応する個人識別番号を探索し、得られた個人識別番号をICカード110に返送する。ステップ1802で、ICカードはデータ鍵生成処理2を行なう。これは、後述する図20のステップ2001以降の処理であり、個人識別番号のチェックやデータ鍵を生成する処理である。

【0093】図19は、本実施例において、記憶装置200に記憶されている暗号文ファイルを読み取り、それを復号する場合の処理手順を示す流れ図である。これは基本的に図9と同じである。ただし、図18と同様に、図9のステップ904がステップ1800、1801、1802に置き替わっている。すなわち、識別番号テーブル1600を参照することにより、ICカードから受け取ったカード識別番号と対応する個人識別番号を探索し、得られた個人識別番号をICカードに返送して、個人識別番号のチェックを行なう点が異なる。

【0094】図20は、ファイルの書き込み及び読み取り時のICカード内部の鍵生成処理を示す流れ図である。これは基本的には図15と同じである。ただし、ステップ2000、2001が付け加えられている点がある。

【0095】すなわち、端末から鍵生成権リストを受け

取ったら、まず、カード識別番号を端末100に送る（ステップ2000）。このステップ2000は、図18、19のステップ1800に対応する。図18、19で説明したように、端末は、ICカードから受け取ったカード識別番号と対応する個人識別番号をICカードに送る。ICカードは、返送されてきた個人識別番号と自カード内の個人識別番号とが一致するかどうかのチェックを行なう（ステップ2001）。

【0096】本実施例によれば、第1から第3の実施例と同様の効果が得られるほかに、ユーザが位置するノード（役職）に変更があった場合（このとき、その変更に応じて記憶装置内の識別番号テーブルが書き替えられている）に、以前のユーザにはファイルを復号できなくなることが可能であり、安全性や拡張性を増すことができる。

#### 【0097】

【発明の効果】以上説明したように、本発明の暗号方式によれば、ファイル共有を行なうユーザが所有するICカードなどの記憶媒体の識別番号を使って暗号鍵を生成するので、複数ユーザによって共有されるファイルを適式に暗号化することができ、情報の安全性を高めることができる。また、自分より下位階層のユーザのマスタ鍵をすべて持つようにしなくてもよいので、ユーザの負担が軽減される。

【0098】さらに、上記ICカードなどの記憶媒体の識別番号を、ユーザ階層に即した形で設定しているので、ある階層に属するユーザによって管理されている暗号化された情報を、その上位階層に属するユーザも正しく復号することができる。

#### 【図面の簡単な説明】

【図1】本発明の第1の実施例を示すブロック図である。

【図2】第1の実施例のシステム構成図である。

【図3】第1の実施例における端末の内部構成図である。

【図4】第1の実施例におけるICカードの内部構成図である。

【図5】第1の実施例におけるユーザ及びマスタ鍵の構成図である。

【図6】第1の実施例における識別番号テーブルの構成図である。

【図7】第1の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図8】第1の実施例において、平文ファイルを暗号化する場合のICカード内部の処理を示す流れ図である。

【図9】第1の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

【図10】第1の実施例において、暗号文ファイルを復号する場合のICカード内部の処理を示す流れ図である。

【図 1 1】本発明の第 2 の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図 1 2】本発明の第 3 の実施例を示すブロック図である。

【図 1 3】第 3 の実施例における階層別マスタ鍵の生成方法を示すブロック図である。

【図 1 4】第 3 の実施例における IC カードの内部構成図である。

【図 1 5】第 3 の実施例における IC カード内部の処理を示す流れ図である。

【図 1 6】本発明の第 4 の実施例を示すブロック図である。

【図 1 7】第 4 の実施例における IC カードの内部構成図である。

【図 1 8】第 4 の実施例において、平文ファイルを暗号化する場合の処理手順を示す流れ図である。

【図 1 9】第 4 の実施例において、暗号文ファイルを復号する場合の処理手順を示す流れ図である。

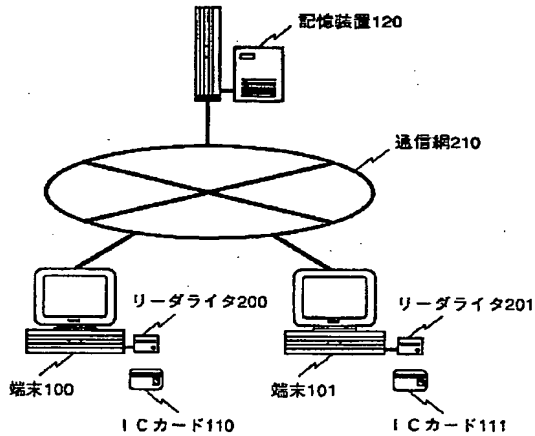
【図 2 0】第 4 の実施例における IC カード内部の処理を示す流れ図である。

【図 2 1】役職によって階層化されたユーザの構成を示す図である。

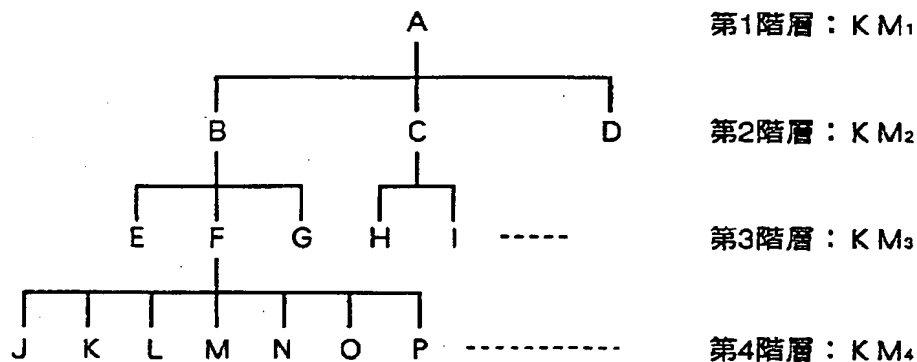
【符号の説明】

100、101…端末、  
110、111…IC カード、  
120…記憶装置、  
200、201…リーダライタ、  
210…通信網。

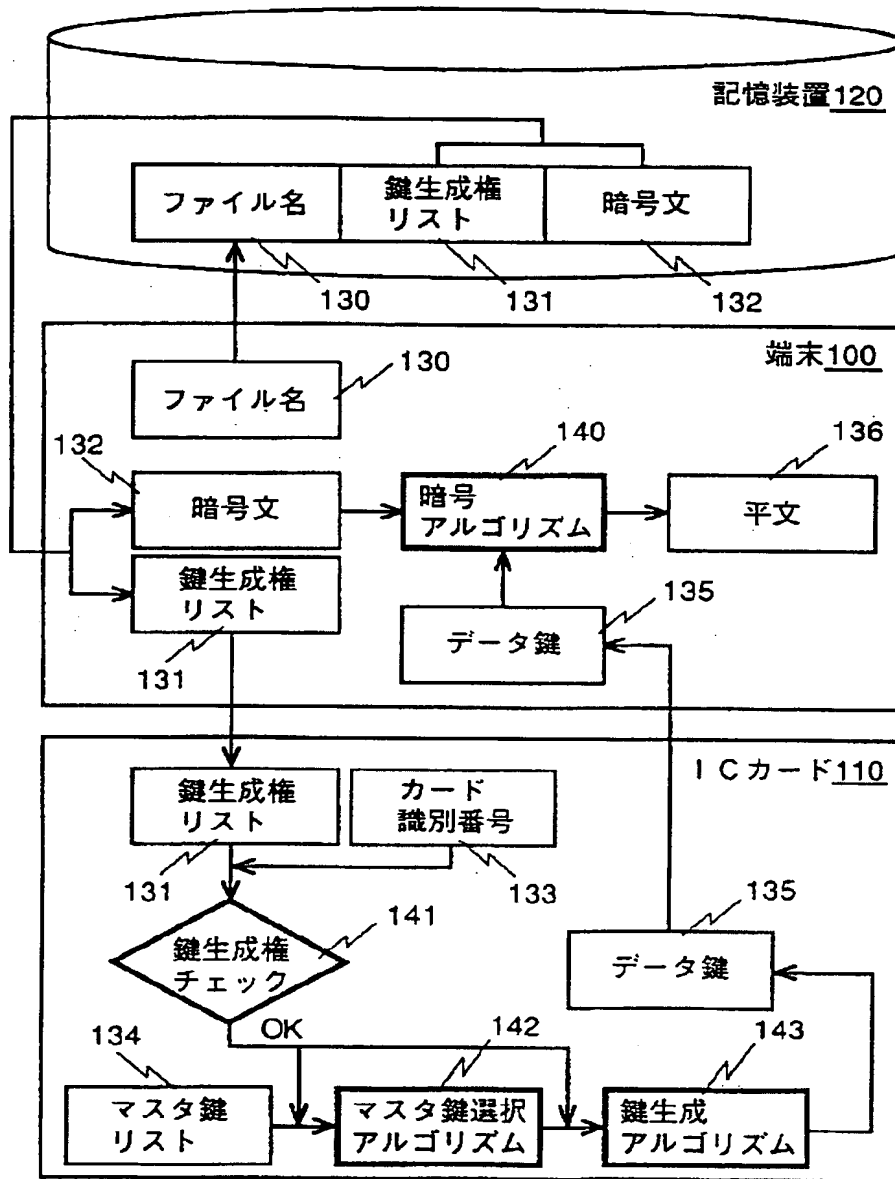
【図 2】



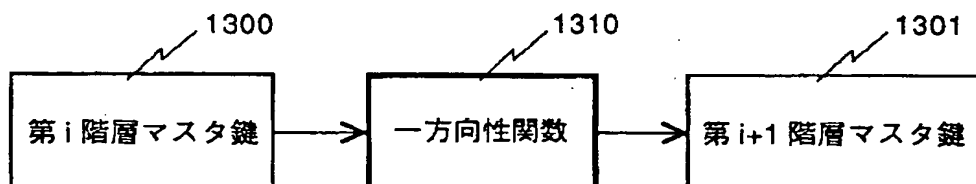
【図 5】



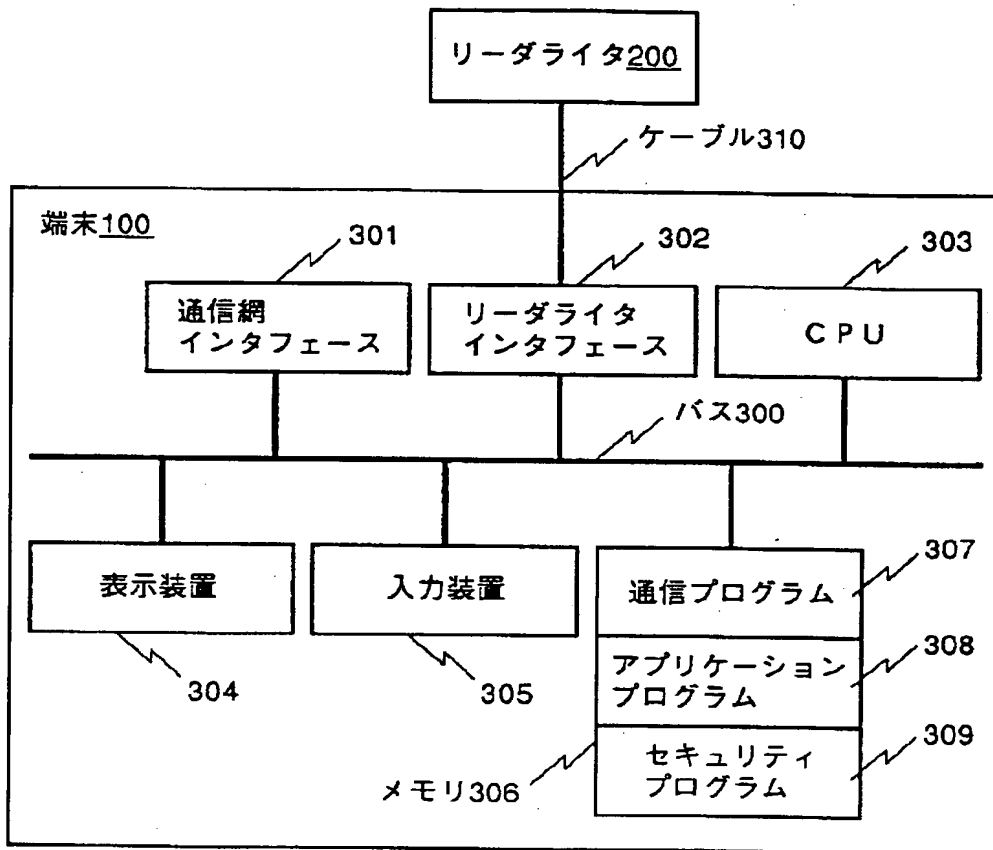
【図1】



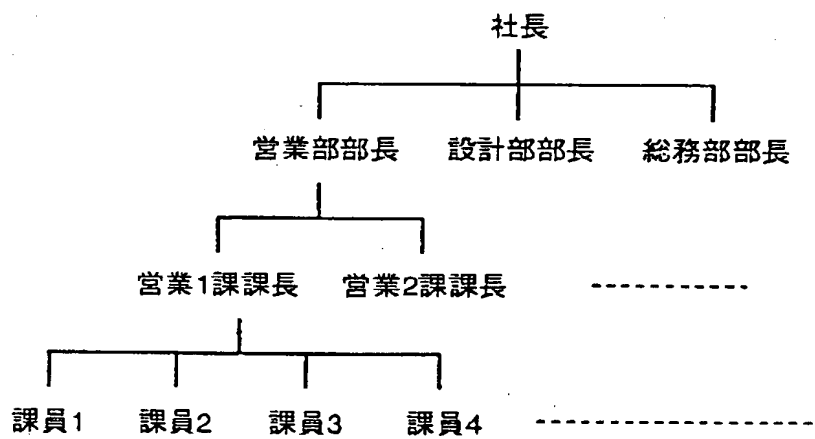
【図13】



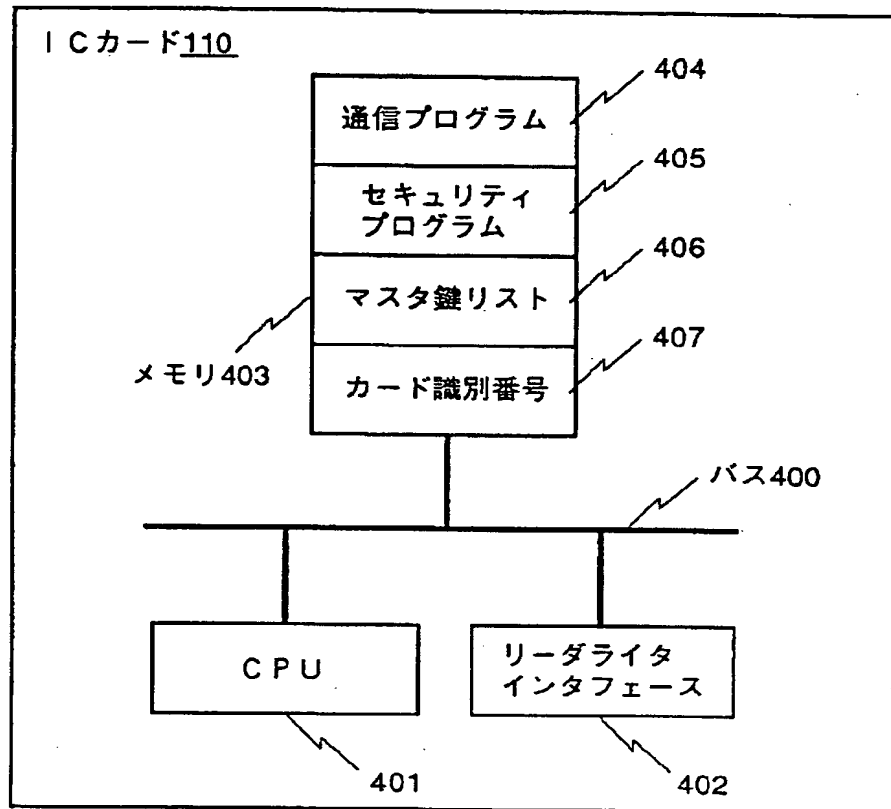
【図 3】



【図 2 1】



【図4】

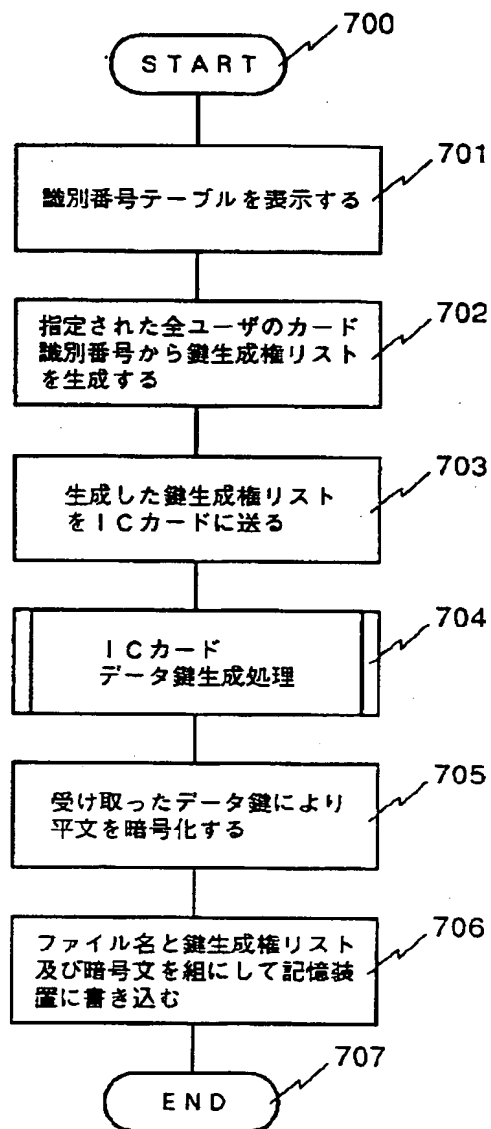


【図 6】

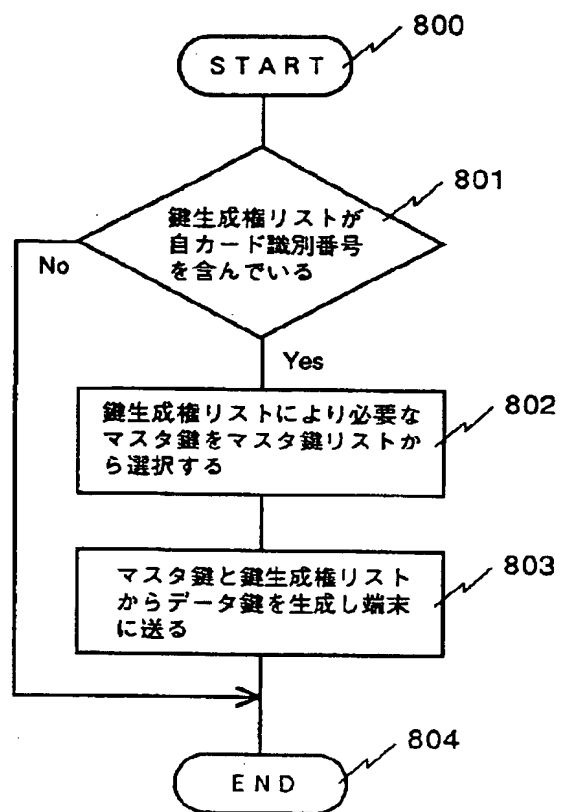
氏名	役 職	個人識別番号	カード識別番号
A	所長	67040m	(1,0,0,0)
B	第1部長	72071m	(1,1,0,0)
C	第2部長	72019m	(1,2,0,0)
⋮	⋮	⋮	⋮
G	第1部第3課長	79001m	(1,1,3,0)
H	第2部第1課長	77038m	(1,2,1,0)
⋮	⋮	⋮	⋮
L	第2部第1課員	89107f	(1,1,2,3)
M	第2部第1課員	90005f	(1,1,2,4)
N	第2部第1課員	90022m	(1,1,2,5)
⋮	⋮	⋮	⋮

識別番号テーブル600

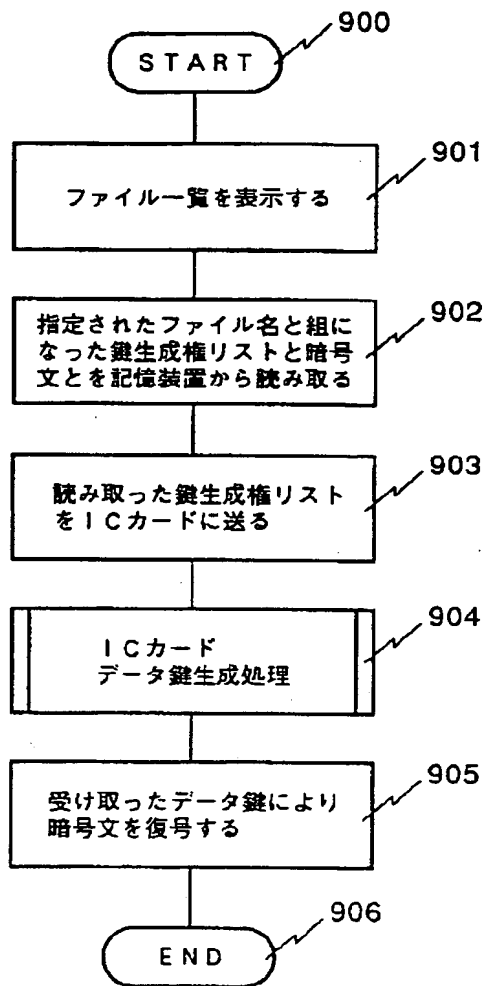
【図 7】



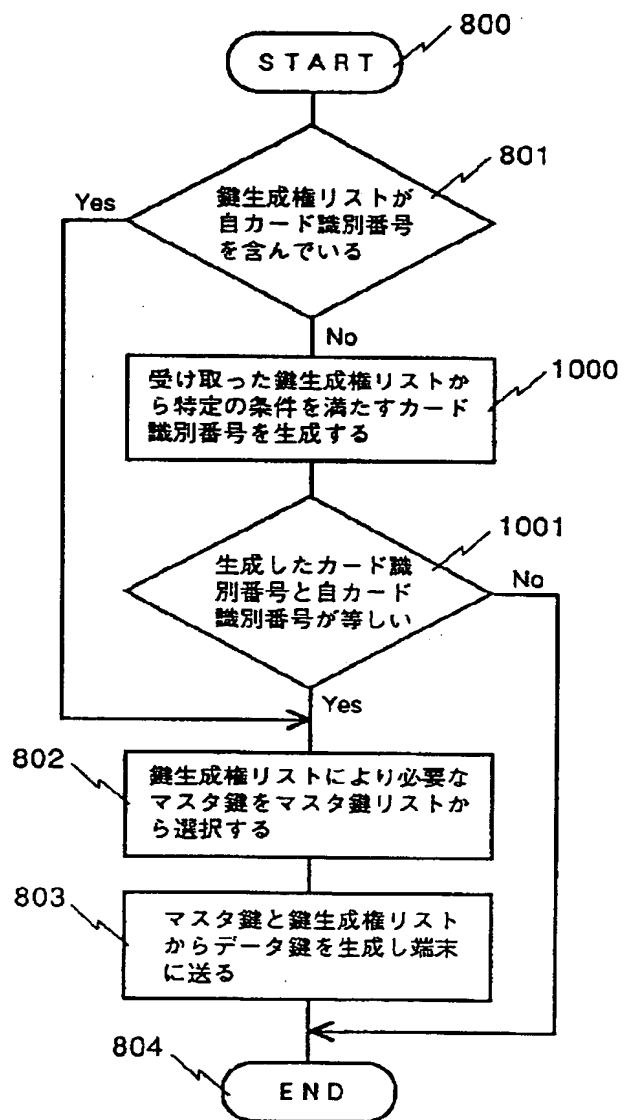
【図 8】



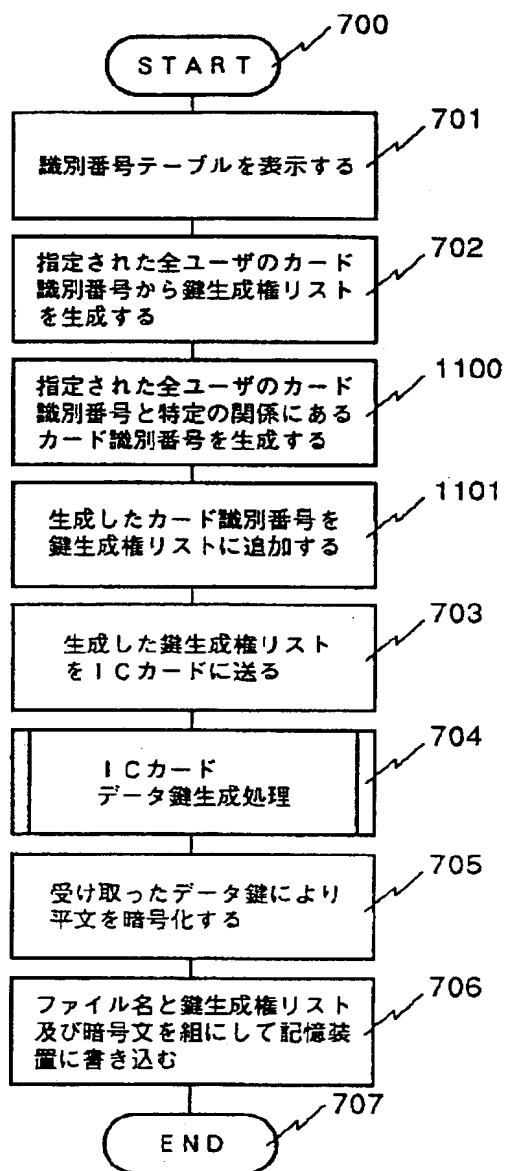
【図9】



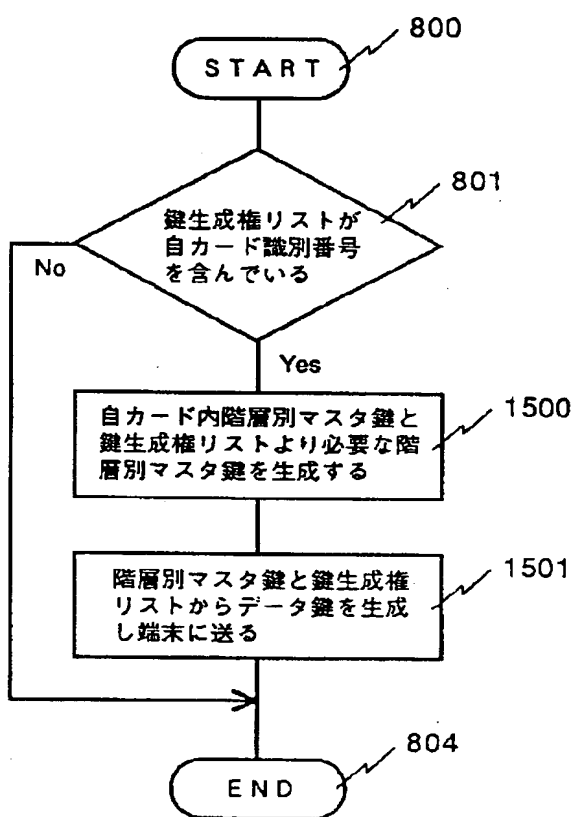
【図10】



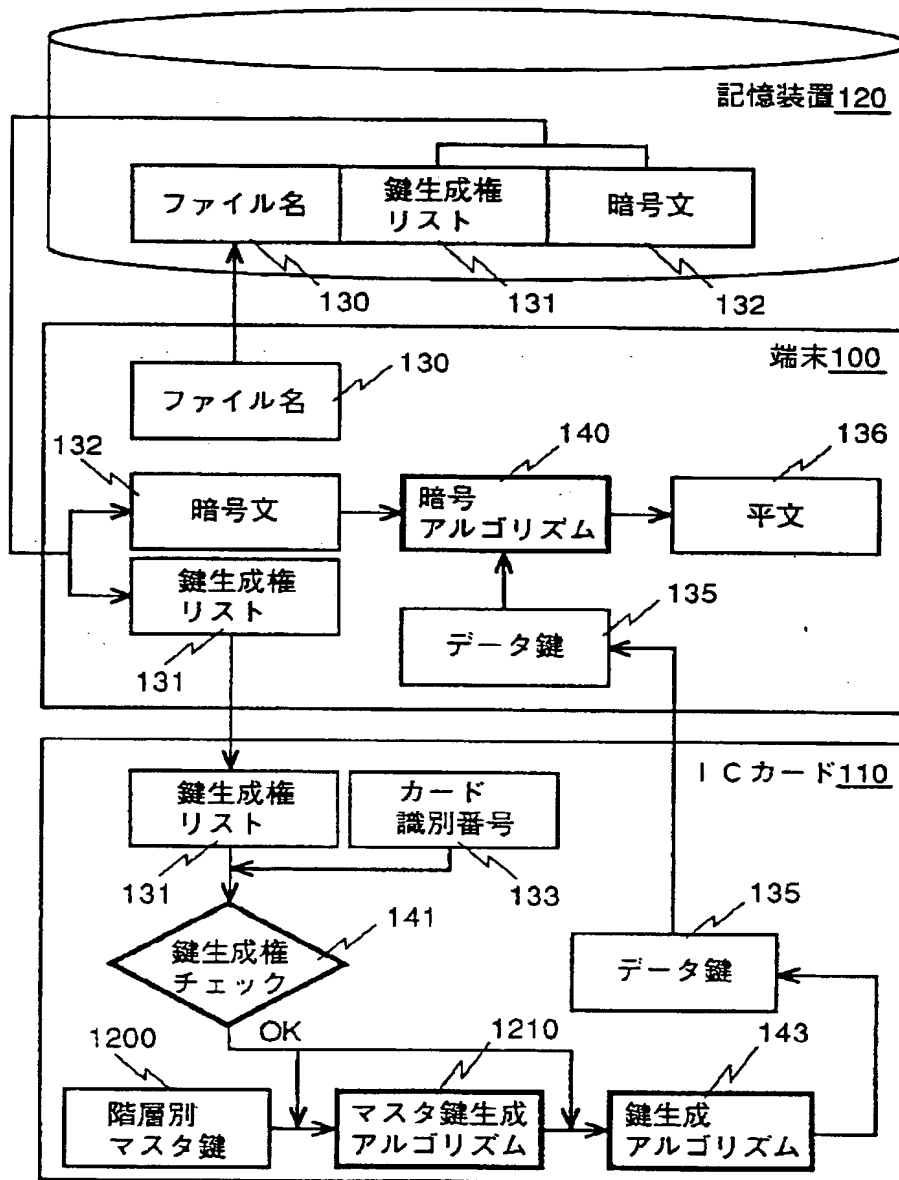
【図 11】



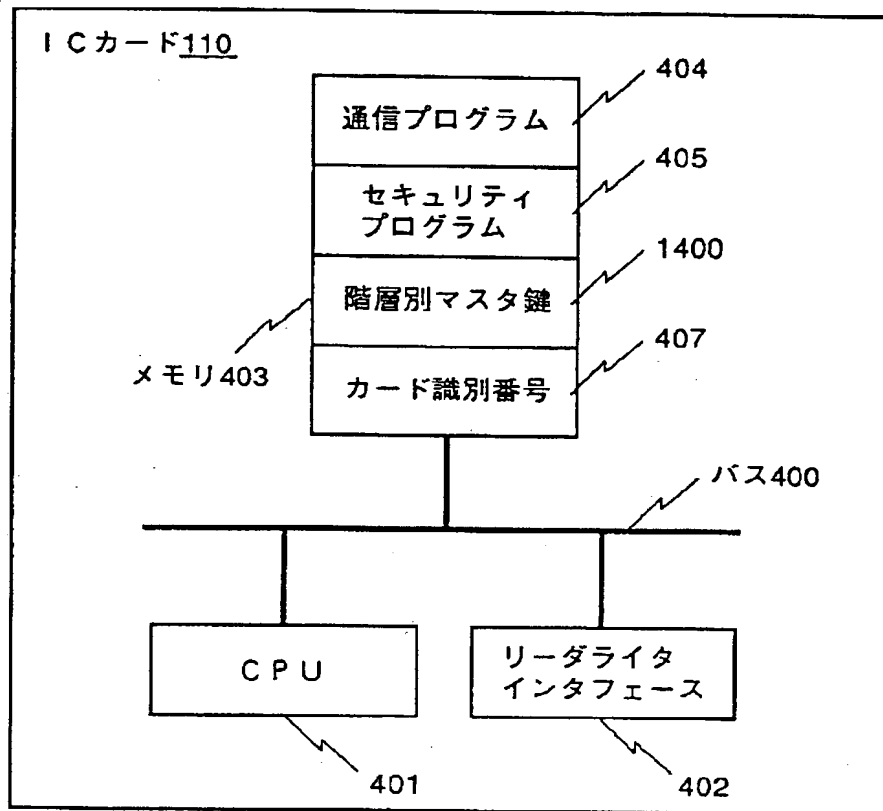
【図 15】



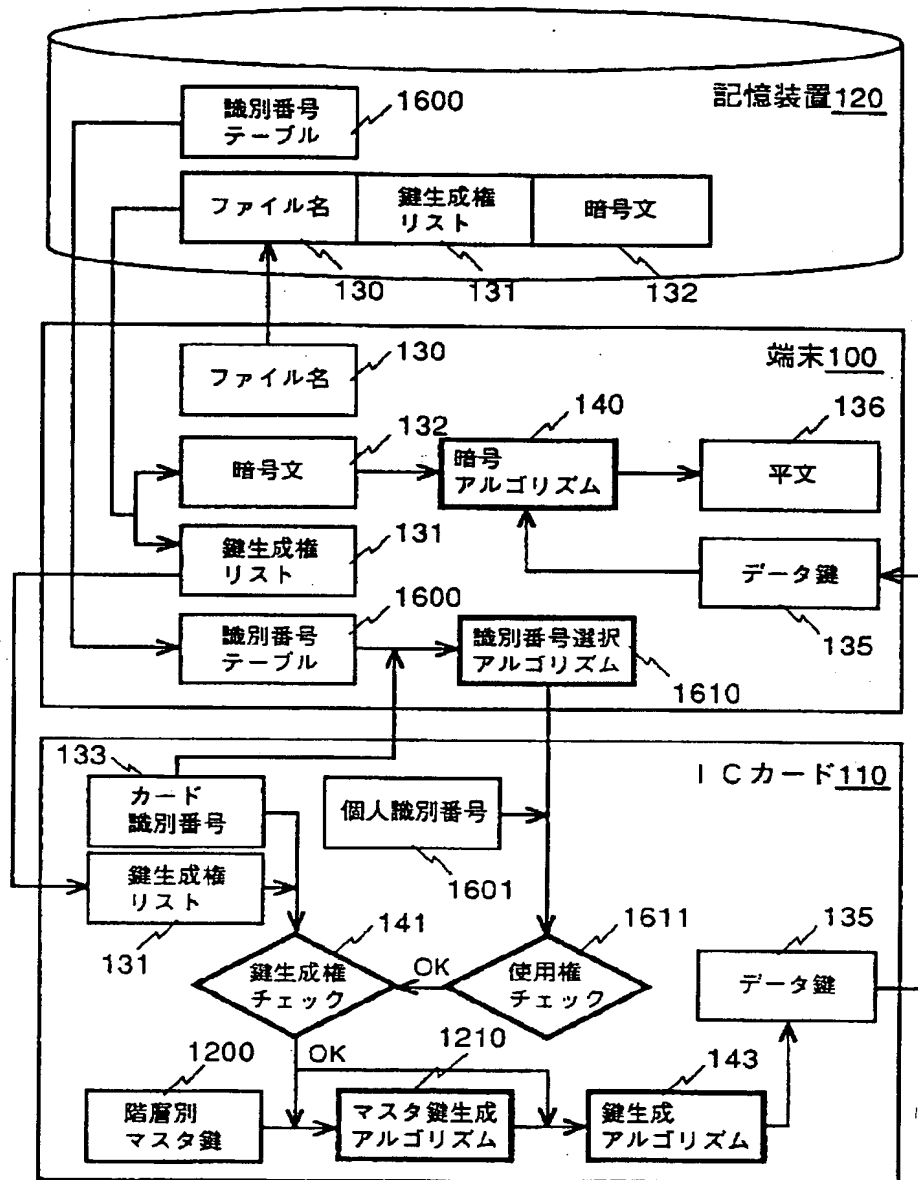
【図12】



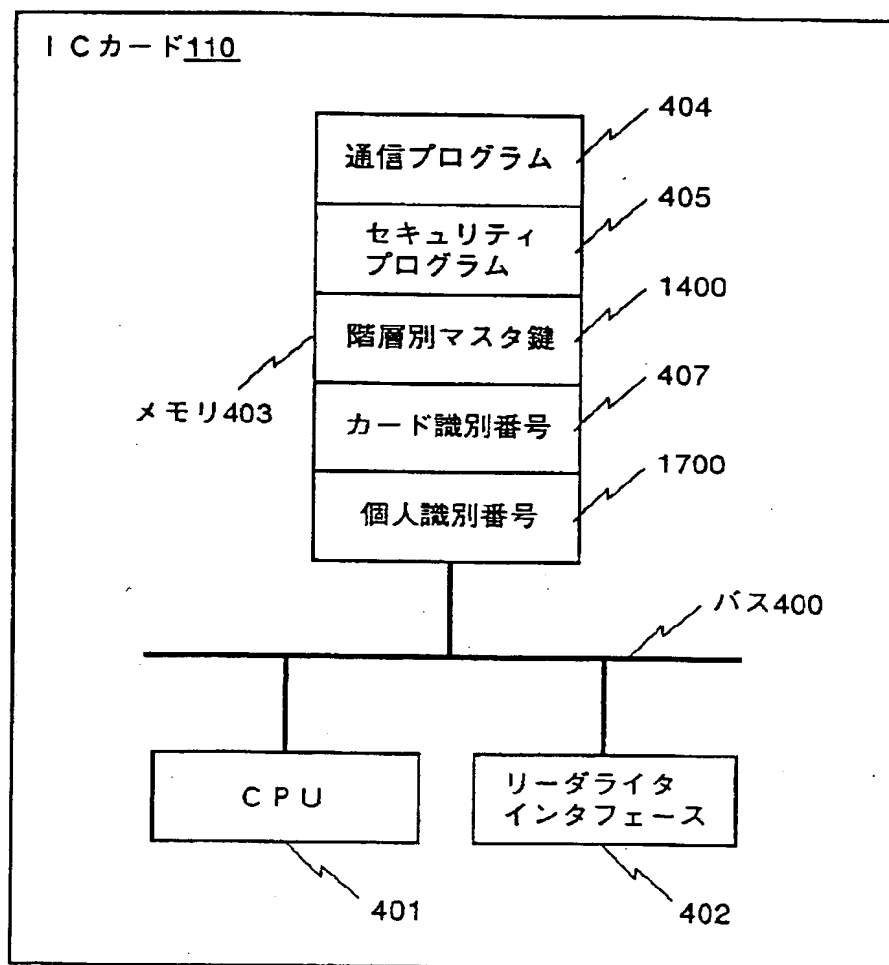
【図14】



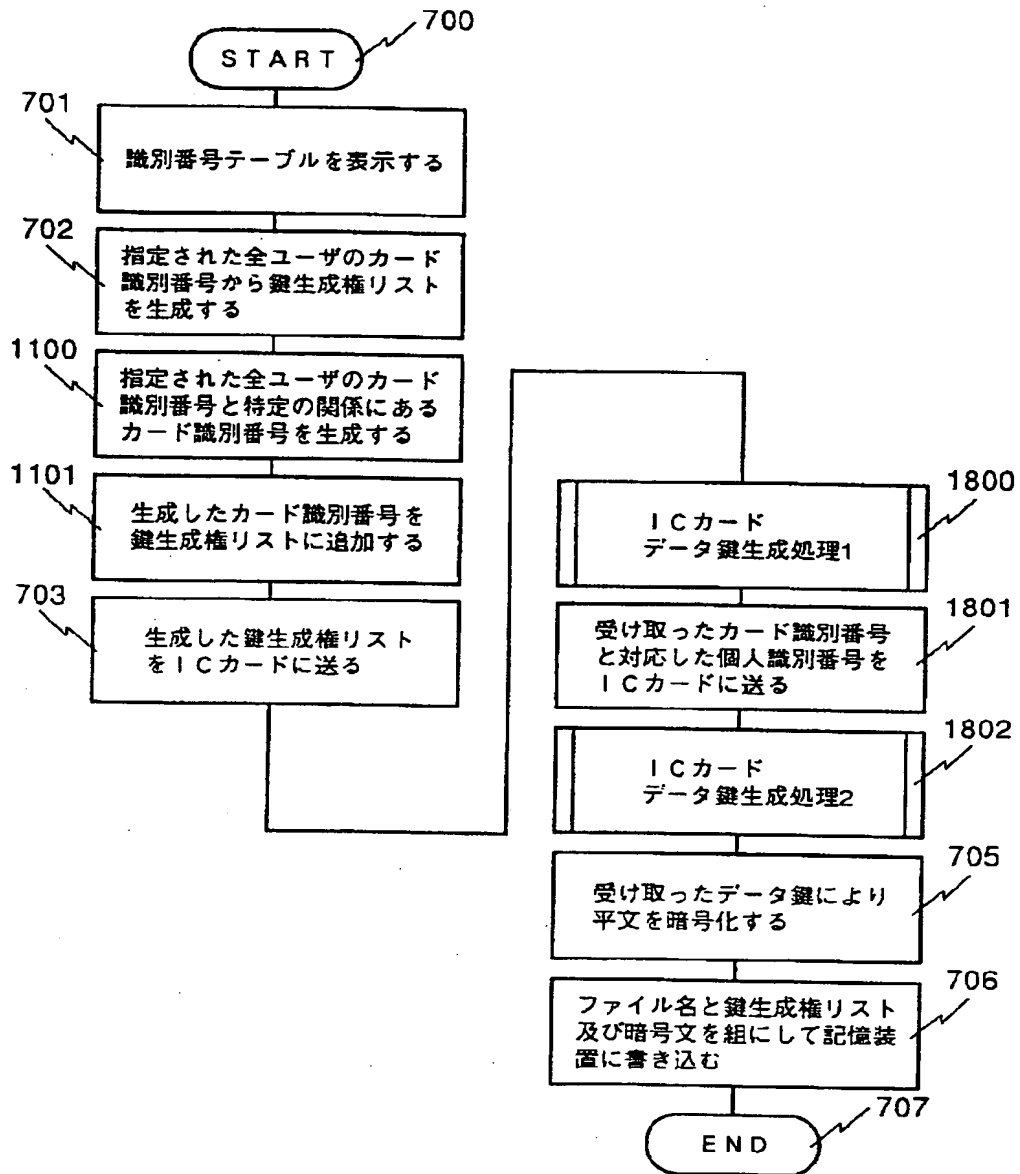
【図16】



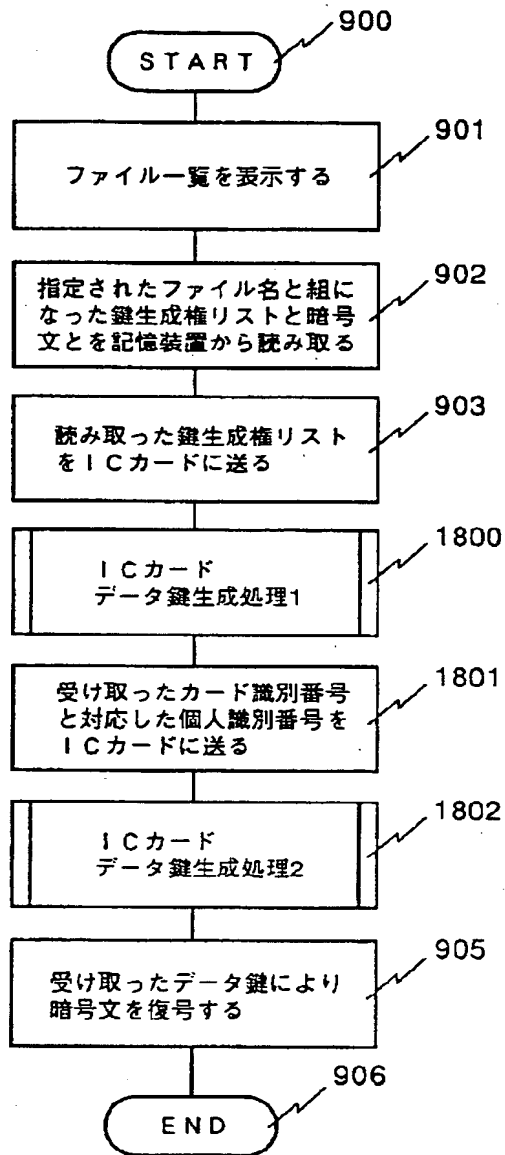
【図 1 7】



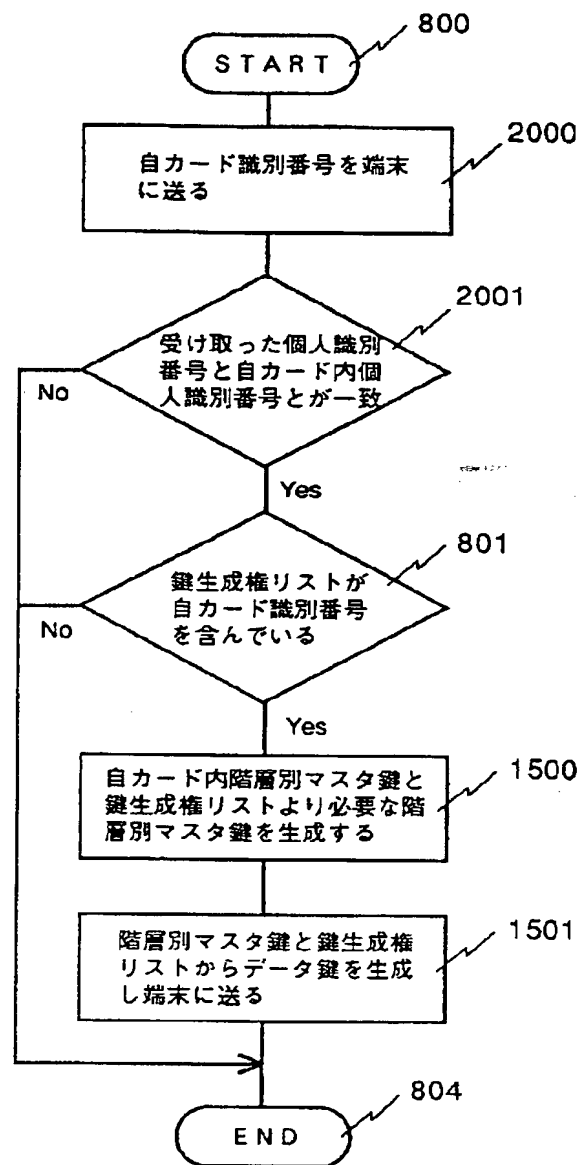
【図18】



【図 19】



【図 20】



フロントページの続き

(72)発明者 松本 浩

愛知県名古屋市中区栄三丁目10番22号 日  
立中部ソフトウェア株式会社内